

Secure Web Applianceのスマートライセンスの トラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[シスコスマートライセンス](#)

[Smart Software Managerサテライト](#)

[スマートライセンスに関連する定義](#)

[Secure Web Applianceでのスマートライセンスの設定](#)

[はじめる前に](#)

[CLIおよびGUI表示の変更](#)

[リセットとリロード](#)

[通信の要件](#)

[GUIからのスマートライセンスの設定](#)

[統合の検証](#)

[GUIからのスマートライセンスステータスの確認](#)

[CLIからのスマートライセンスステータスの確認](#)

[スマートライセンスポータルでのデバイスステータスの確認](#)

[CLIからのVLNの検索](#)

[Logging](#)

[トラブルシューティングスマートライセンス](#)

[持続的な接続](#)

[Registration failed](#)

[通信送信エラー](#)

[トークンが無効です](#)

[承認を更新できませんでした](#)

[通信送信エラー](#)

[証明書が失効している](#)

[デバイスにVLNがない](#)

[スマートライセンスエージェントサービスは利用できません](#)

[署名を確認できませんでした](#)

[Smart agentが無効状態でスタックしている](#)

[スマートエージェントサービスの初期化に失敗しました](#)

[ライセンスクラウドからの応答が無効です](#)

[有効なSSL証明書が送信されませんでした](#)

[機能はコンプライアンス違反に移行されました](#)

[スマートエージェントが認証期限切れ状態](#)

[参考](#)

はじめに

このドキュメントでは、セキュアWebアプライアンス(SWA)でスマートライセンスを設定およびトラブルシューティングする手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- スマートライセンスの機能
- Secure Web Appliance(SWA)の管理。

Cisco では次の前提を満たす推奨しています。

- インストールされている物理または仮想のセキュアWebアプライアンス(SWA)。
- SWAへの管理アクセス。
- スマートライセンスポータルへのアクセス

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

シスコスマートライセンス

スマートライセンスは、次の機能を提供します。

- すべての製品ライセンスを一元管理
- ライセンスの適用と管理に1つの方法を使用して、物理および仮想Eメールセキュリティアプライアンス(ESA)/セキュリティ管理アプライアンス(SMA)/SWA間のプロセスを標準化
- ライセンスをESA/SMA/SWAに簡単に適用
- ライセンスの期限切れに関するアラートを受信
- ハードウェアモデルのESA/SMA/SWAには、購入後すぐに、すべてのサービスを対象とした90日間の評価期間があります

SWAをスマートライセンスに登録するには、アプライアンスの所有者にスマートアカウントが必要です。

- スマートアカウントは、ドメインごとに1つずつ発行されます。

- スマートアカウントの管理者は、リソースの分離を可能にするサブレベルの仮想アカウントを作成できます。
- 仮想アカウントを使用すると、必要に応じて異なるシスコ製品ライセンスへのアクセスを制限できます。
- Cisco Smart Software Manager(CSSM)にアクセスして、ライセンスを管理し、トークンをダウンロードします。

シスコが提供するリソースへのリンクには、スマートライセンスに関連するビデオ、ガイド、および説明が含まれます。

- [新しいスマートアカウントの作成または既存のアカウントへのユーザの追加要求](#)
- [スマートソフトウェアライセンスの概要Cisco Webページ](#)
- [スマートライセンス導入ガイド](#)
- [シスコスマートアカウントのシスコページ](#)
- [Smart Software Managerに関するシスコページ](#)
- [Cisco Smart Software Manager\(CSSM\)](#)
- [Eメールセキュリティ用のPAKファイルからのライセンスキーファイルの生成 - シスコ](#)

Smart Software Managerサテライト

Cisco Smart Software Managerサテライトは、Cisco Smart Licensingのコンポーネントです。

CSSMサテライトは、CSSMと連携して製品ライセンスを管理し、使用中のCiscoライセンスをほぼリアルタイムに可視化してレポートします。

セキュリティ上の理由から、Cisco.comにあるSmart Software Managerを使用してインストールベースを管理したくない場合は、Smart Software Managerサテライトを社内にインストールすることもできます。

Smart Software Mangerサテライトの詳細については、[Cisco Smart Software Manager - Cisco](#)を参照してください。

スマートライセンスに関連する定義

ライセンスのタイプ:

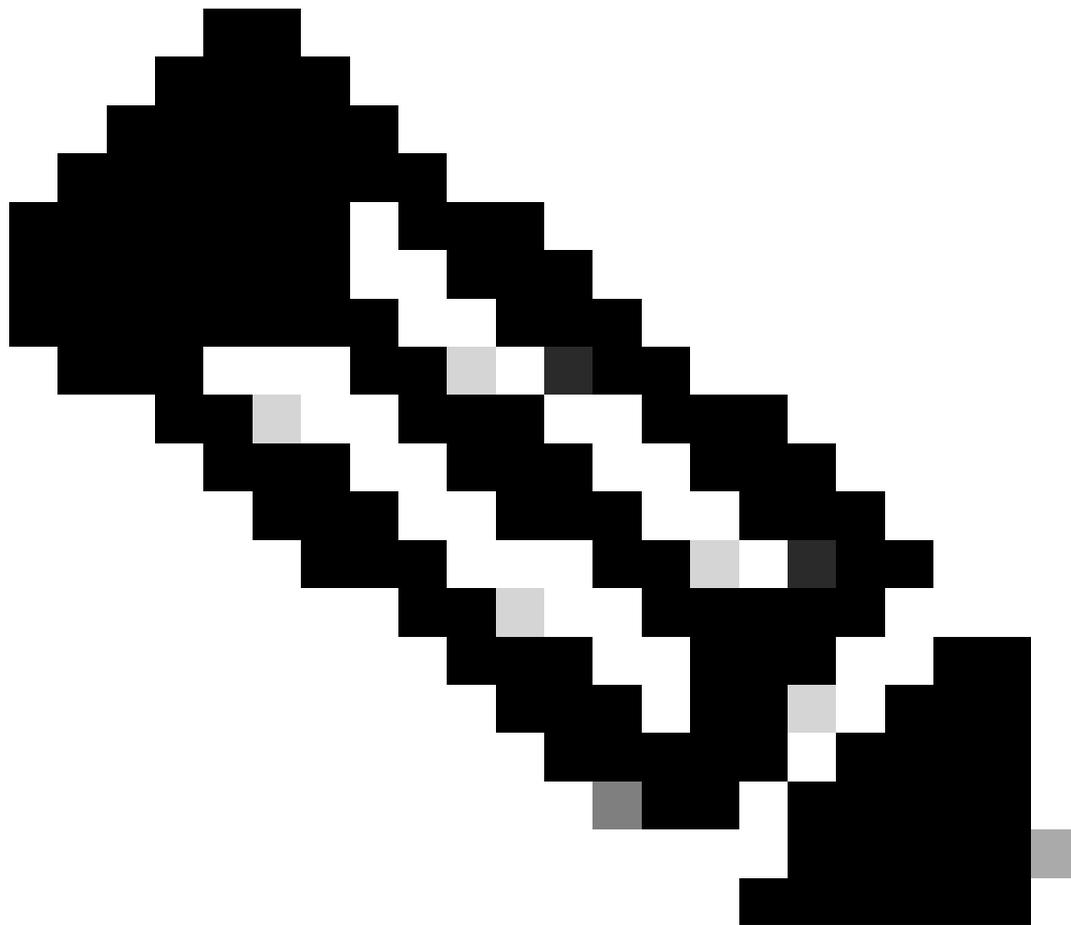
- クラシックライセンス(CL)は、ハードウェアと仮想の両方のライセンスに使用される従来の方法を指します。
- スマートライセンス(SL)

ライセンス認証ステータス：アプライアンス内の特定のライセンスのステータス。

- ESA/SWA/SMAでは、スマートライセンスページに実際の有効期限は表示されません。
- 場所：GUI > System Administration > Licenses
- 場所：CLI > license_smart > SUMMARY

特定の機能のステータスは、次のいずれかの値で表示されます。

- 評価:
 - SLサービスがトークン登録なしで新しい (ハードウェア) ESA/SMAで有効になりました
 - 現在のCLがインストールされているアプライアンスでSLサービスが有効になっている
- Eval Expired:90日間評価版スマートライセンスの有効期限が切れ、アプライアンスは追加の30日間猶予期間に移行しました。
- 準拠 : アプライアンスはトークンで登録されており、現在、この機能は有効なライセンスを消費します
- コンプライアンス違反 (猶予期間) は、次の2つのシナリオで確認できます。
 - 一時的な30日間の機能ライセンスのワンクリック要求が使用中です
 - アプライアンスのライセンスが期限切れになり、30日の猶予期間が開始されました
- コンプライアンス違反 (期限切れ) : ライセンスが完全に期限切れになり、関連サービスが機能しなくなります



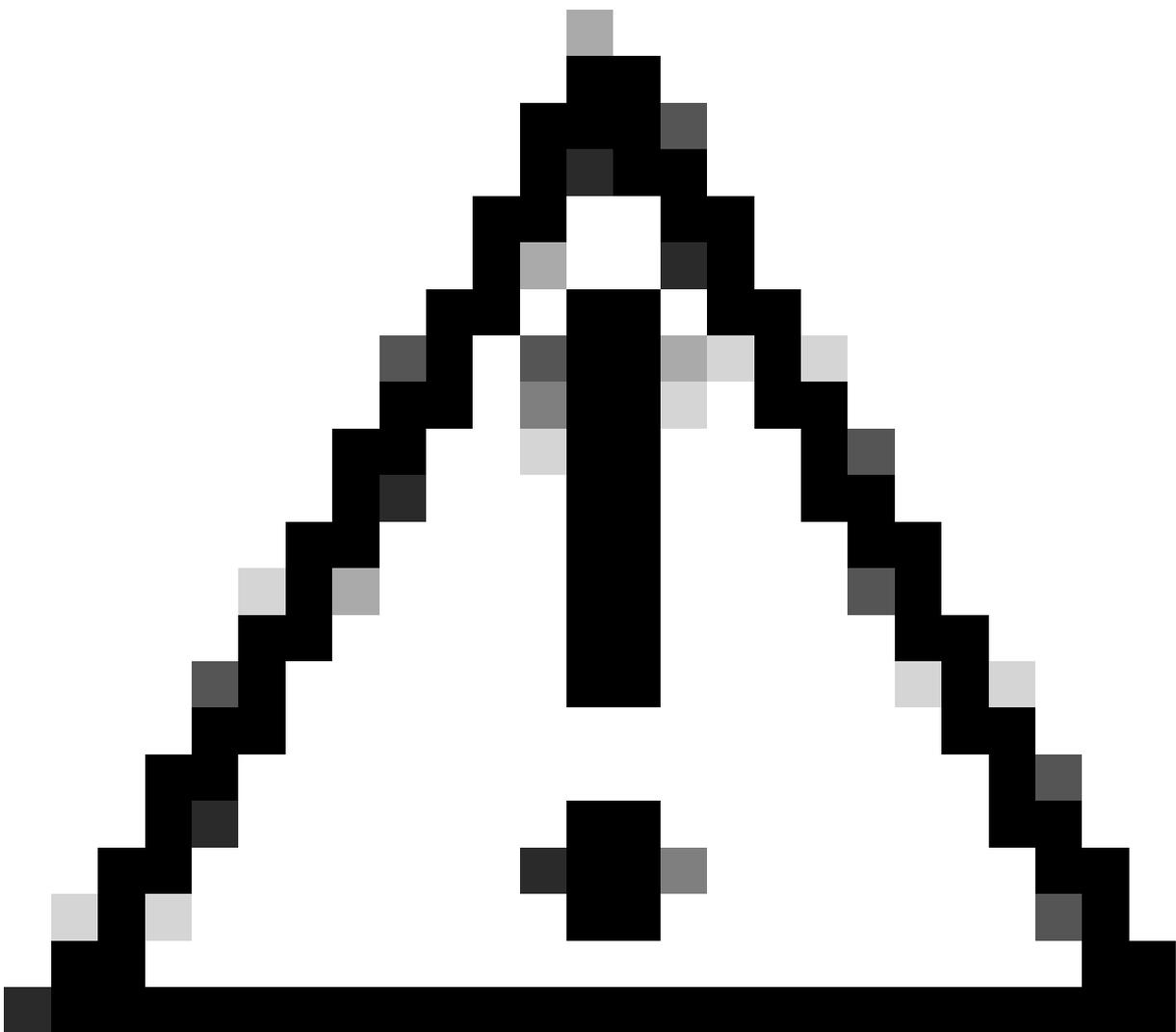
注 : Perpetualキーは、その機能に有効期限がないことを示します。休止キーは、機能自体に使用許諾契約書(EULA)があり、そのEULAに同意する必要があること、または機能を

設定して有効にする必要があることを示します。完了すると、機能はアクティブに移行し、有効期限タイマーが開始されます。

Secure Web Applianceでのスマートライセンスの設定

SWAをスマートライセンスに接続するには、グラフィカルユーザインターフェイス(GUI)とコマンドラインインターフェイス(CLI)の両方を使用できます。

はじめる前に



注意:ESA/SMA/SWAでスマートライセンス機能を有効にすることは永続的であり、アップライアンスをクラシックライセンスモードに戻すオプションを使用することはできません。

-
- SWAが購入したすべてのハードウェアモデルには、全機能の90日間の評価ライセンスが含まれます。

まれています。

- 現行のクラシックライセンス(CL)を使用してスマートライセンスに移行したすべてのハードウェアモデルには、90日間の評価ライセンスが付与されます。
- すべての仮想SWAモデルでは、アップグレード/更新サーバにリンクするために、コマンドラインインターフェイス(CLI)のloadlicense コマンドからアプライアンスにロードされるXMLファイルである基本仮想ライセンス(VLN)が必要です。
- すべての仮想SWAモデルは、作成時に90日間のライセンスが含まれないため、クラシックライセンスのVLN(XMLとも呼ばれる)ファイルによる登録が必要です。
- 現行のクラシックライセンス(CL)で移行するすべての仮想SWAモデルには、90日間の評価ライセンスが含まれています。
- 現在、SWAには、オプション機能としてすべてのリリースビルドでスマートライセンスがあります。
- スマートライセンスを有効にすると、そのボックスでは従来のライセンスは使用されません。
- スマートライセンスを有効にすると、従来のライセンスを保持できなくなります。
- SWAバージョン15.0以降のリリースビルドでは、従来のライセンスを有効にせずにスマートライセンスを直接有効にするオプションがあります。この場合、ライセンスを購入し、スマートライセンスでSWAを使用するように設定する必要があります。
- 15.0リリースのビルドからは、Classic Licenseのアクティベーションを行わずにスマートライセンスを新規インストールおよび登録できる30日間の猶予期間があります。
- 15.1リリースの最新リリースビルドでは、SWAを有効にして正常に機能させるために、スマートライセンスが必須です。また、最新リリースでは、従来のライセンス関連の機能がすべて削除されています。
- スマートライセンスへのアップグレードは、基本ビルドでスマートライセンスが有効になっていない場合、ダウンロード時にSWAの必須ビルドが制限されます。

CLIおよびGUI表示の変更

ClassicライセンスのCLIでは、4つのコマンドを使用しました。そのため、スマートライセンスの委任状ビルド(15.1以降)では、これらのコマンドは削除されます。

削除されたCLIコマンドのリスト：

- ライセンスのロード
- 表示ライセンス
- 機能キー
- 機能キー設定

Classic LicenseのGUIでは、System Administrationタブに2つのページが示されています。したがって、スマートライセンスの委任状では、ページが削除されます。

削除されたGUIページのリスト：

- 機能キーの設定
- 機能キー

リセットとリロード

SWAでの設定のリセットとは、工場出荷時のリセットを実行することです。このリセットでは、設定全体が消去され、SWAが工場出荷時の状態に戻ります。

スマートライセンスでは、構築の権限も同じ動作が維持されます。

ReloadはCLIの隠しコマンドで、設定データを消去し、機能キーも削除します。SWAがクラシックライセンスに登録され、リロードを実行した場合は、ライセンスを再ロードします。

スマートライセンスでSWAが設定されている場合、リロード後にスマートライセンスの登録が解除され、無効になります。また、現在のSWAの動作では工場出荷時の状態にリセットされます。

SWAの必須ビルドバージョンでは、スマートライセンスがdisable状態に戻ることはないため、reloadコマンドですべての設定が消去されます。

スマートライセンスはregistered状態のままであるため、すべてのライセンスを再度要求します。

通信の要件

TCPポート443でのsmartreceiver.cisco.comへのネットワーク通信またはプロキシ通信。

SWAからの接続をテストするには、次の手順を使用します。

ステップ 1 : CLIにログインします。

ステップ 2 : telnetと入力してEnterキーを押します。

ステップ 3 : スマートライセンスサーバへのSWA接続を想定しているインターフェイスを選択します。

ステップ 4 : smartreceiver.cisco.comと入力してEnterを押す。

ステップ 5 : ポートセクションに443と入力し、Enterキーを押します。

注：Smart Software Mangerサテライトを設定している場合は、ステップ4でそのサーバに関連付けられているUniform Resource Locator(URL)またはInternet Protocol(IP)アドレスを追加してください。

正常な接続の例を次に示します。

```
> telnet
```

```
Please select which interface you want to telnet from.
```

1. Auto
2. Management (10.48.48.184/24: management.swa1.cisco.com)
3. P1 (192.168.13.184/24: p1.swa1.cisco.com)
4. P2 (192.168.133.184/24: p2.swa1.cisco.com)

```
[1]> 4
```

```
Enter the remote hostname or IP address.
```

```
[> smartreceiver.cisco.com
```

```
Enter the remote port.
```

```
[23]> 443
```

```
Trying 10.112.59.81...  
Connected to smartreceiver.cisco.com.  
Escape character is '^]'.  
  
^C
```

失敗した接続の例を次に示します。

```
SWA_CLI> telnet
```

```
Please select which interface you want to telnet from.
```

```
1. Auto  
2. Management (10.48.48.184/24: management.swa1.cisco.com)  
3. P1 (192.168.13.184/24: p1.swa1.cisco.com)  
4. P2 (192.168.133.184/24: p2.swa1.cisco.com)  
[1]> 2
```

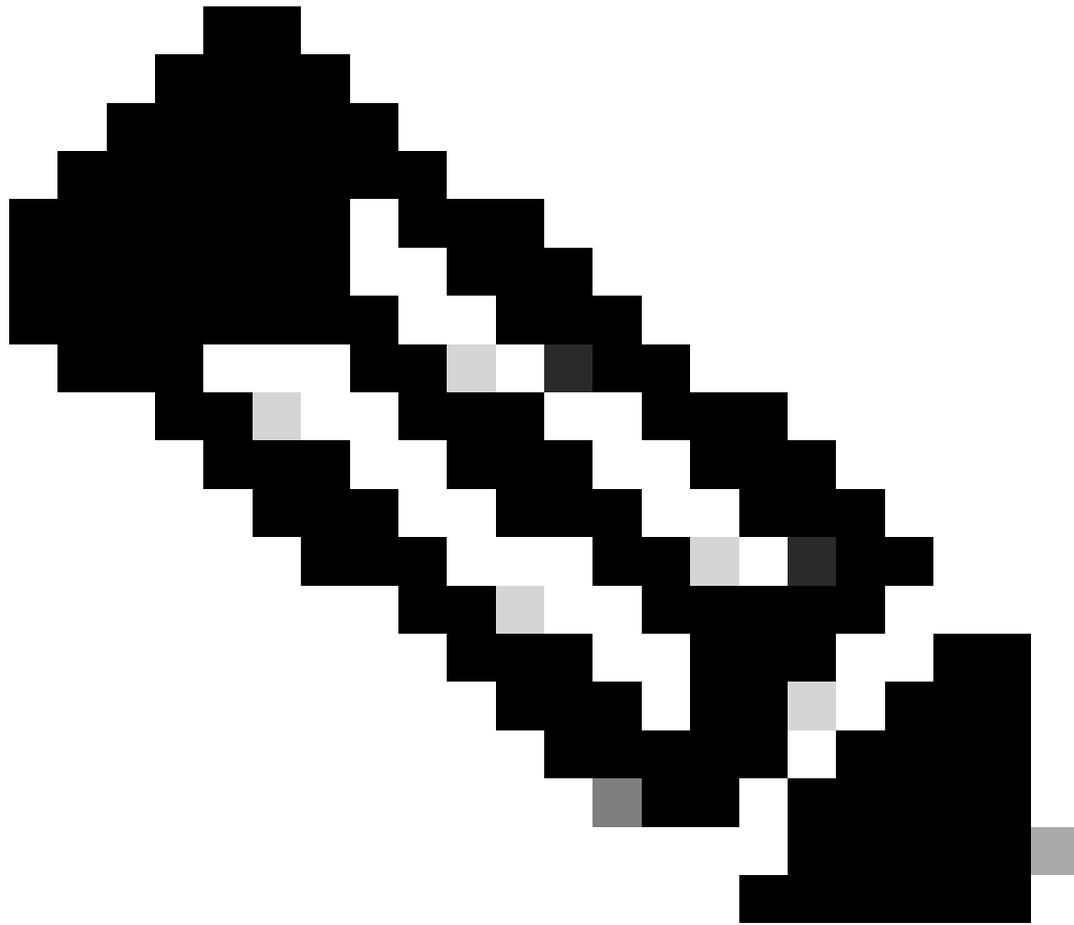
```
Enter the remote hostname or IP address.
```

```
[> smartreceiver.cisco.com
```

```
Enter the remote port.
```

```
[23]> 443
```

```
Trying 10.112.59.81...  
telnet: connect to address 10.112.59.81: Operation timed out  
Trying 2a04:e4c7:fffe::f...  
bind: Invalid argument
```



注：Telnetを終了するには、Ctrl+Cが機能しない場合は、Controlキーを押しながら、]キーを押し、qと入力して、Enterキーを押します。

GUIからのスマートライセンスの設定

ステップ 1： GUIにログインして、System Administrationに移動します。

ステップ 2： Smart Software Licensingを選択します。

System Administration

Policy Trace

Alerts

Log Subscriptions

Return Addresses

SSL Configuration

Users

Network Access

System Time

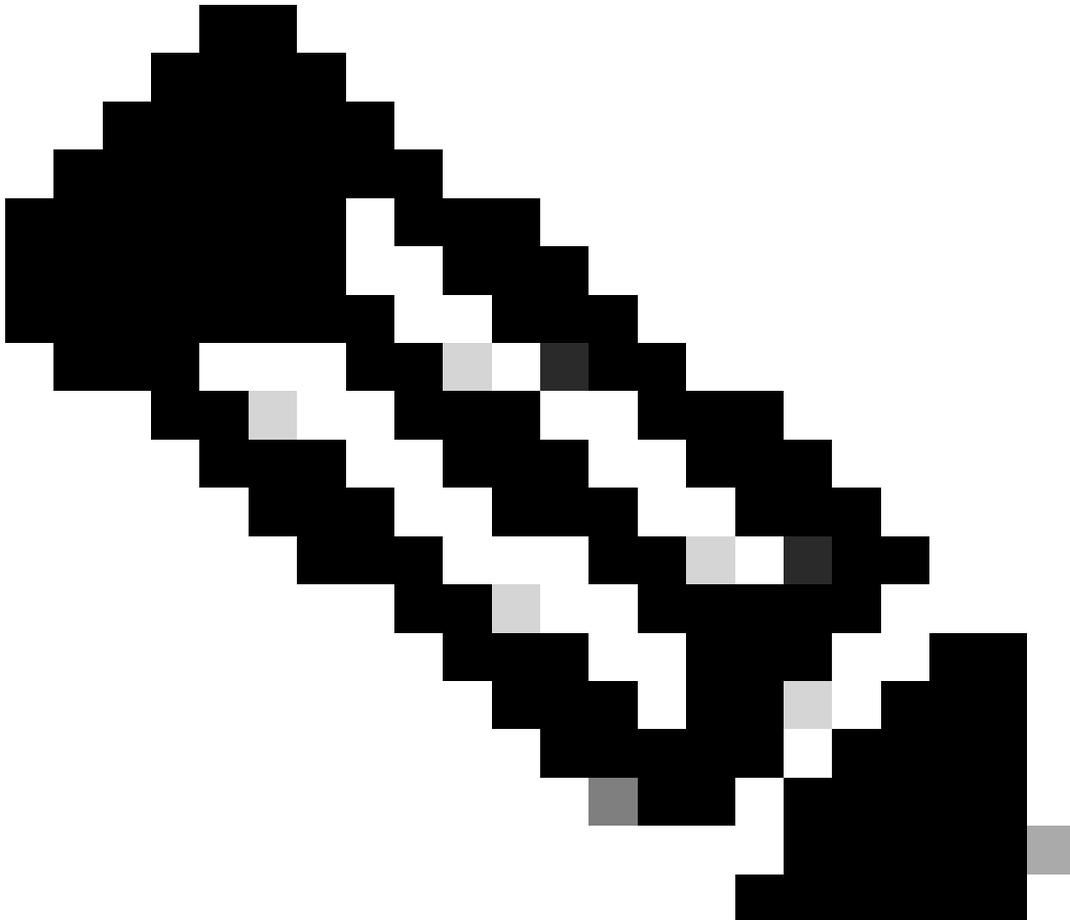
Time Zone

Time Settings

Configuration

Configuration Summary

ステップ 2 : Administration > Manage Smart Account > Virtual Accountsの順に移動します。
ステップ 3 : 対象の仮想アカウントをクリックします。
ステップ 4 : 新しい名前を定義し、英語以外の文字を削除します。



注 : 仮想アカウントの名前を変更するには、管理者権限が必要です。

[2番目のテスト]仮想アカウント名が正しい場合は、デバイスがスマートライセンスポータルインベントリにリストされていることを確認してください。

この記事の「スマートライセンスポータルでのデバイスステータスの確認」の項に記載されている手順を使用します。

[3番目のテスト]デバイスがスマートライセンスポータルインベントリにリストされている場合は、CLIからSWAスマートライセンスサービスを再起動してください。

ステップ 1 : CLIにログインします。

ステップ 2 : diagnosticコマンドを実行します。

ステップ 3 : サービスの選択

ステップ 4 : SMART_LICENSEを選択します

ステップ 5 : RESTARTを選択します。

```
SWA_CLI> diagnostic
```

```
Choose the operation you want to perform:
```

- NET - Network Diagnostic Utility.
- PROXY - Proxy Debugging Utility.
- REPORTING - Reporting Utilities.
- SERVICES - Service Utilities.

```
[> SERVICES
```

```
Choose one of the following services:
```

- AMP - Secure Endpoint
- AVC - AVC
- ADC - ADC
- DCA - DCA
- WBRS - WBRS
- EXTFEED - ExtFeed
- L4TM - L4TM
- ANTIVIRUS - Anti-Virus xiServices
- AUTHENTICATION - Authentication Services
- MANAGEMENT - Appliance Management Services
- REPORTING - Reporting Associated services
- MISCSERVICES - Miscellaneous Service
- OSCP - OSCP
- UPDATER - UPDATER
- SICAP - SICAP
- SNMP - SNMP
- SNTP - SNTP
- VMSERVICE - VM Services
- WEBUI - Web GUI
- SMART_LICENSE - Smart Licensing Agent
- WCCP - WCCP

```
[> SMART_LICENSE
```

```
Choose the operation you want to perform:
```

- RESTART - Restart the service
- STATUS - View status of the service

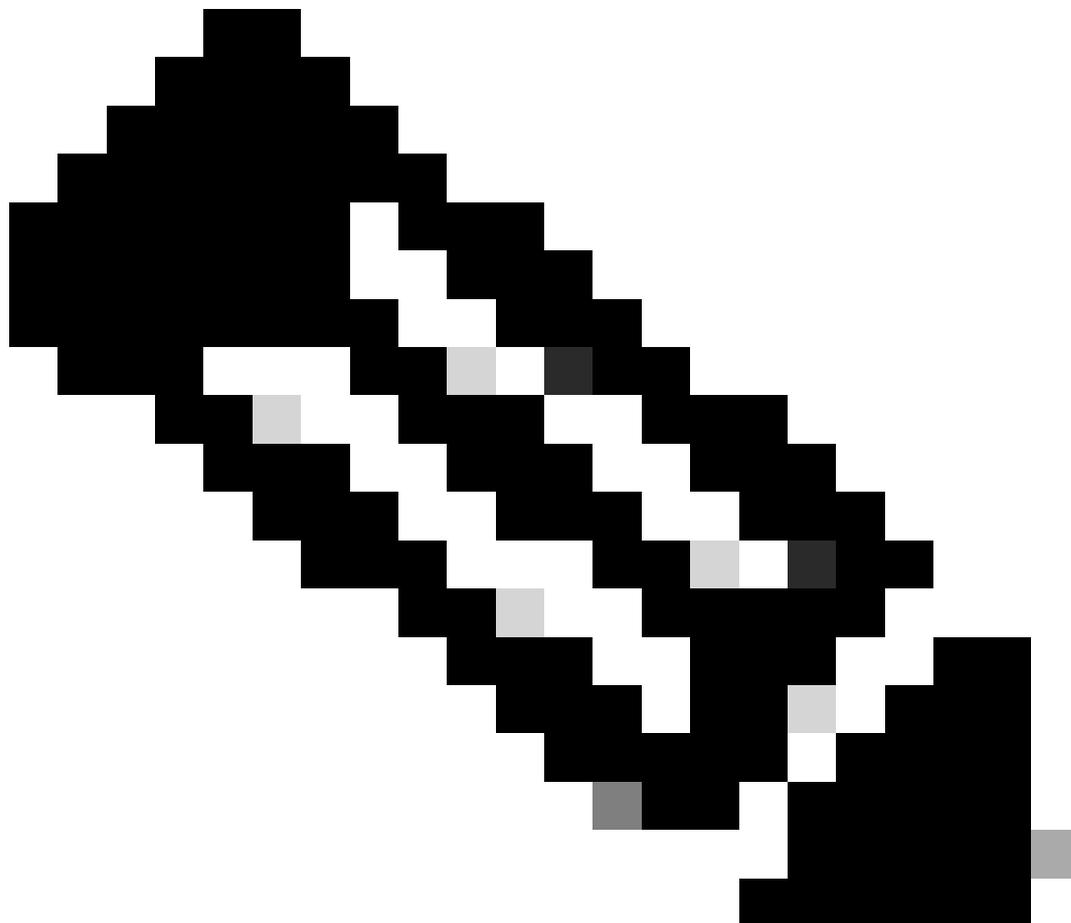
```
[> RESTART
```

```
smart_agent is restarting.
```

[次のテスト] Smart License Managerポータルで新しいトークンを生成し、デバイスを再登録します。

Smart_agentが無効状態でスタックしている

これらのエラーは、アプライアンス（アップグレード前にスマートライセンスが有効になっていた）をバージョン14.1または14.0にアップグレードした後に、ESAまたはSMAで発生する可能性があります。



注：このエラーはx195またはx395デバイスで発生します。

アプライアンスによって生成されるメッセージの例を次に示します

```
08 Apr 2023 10:19:36 -0500 Initialization of smart agent service failed. Reason : Port 65501 is not ava
```

smart_licenseのログには、次の情報が含まれます。

```
Mon Apr 8 09:02:36 2021 Warning: Smart License: Failed to change the hostname to esa.local for the prod
```

このエラーは、ESAのCisco Bug ID [CSCvz74874](#)およびSMAのCisco Bug ID [CSCvx68947](#)が判明していることが原因です。この問題を解決するには、シスコサポートにお問い合わせください。

スマートエージェントサービスの初期化に失敗しました

このエラーは、想定よりも多くのリソースを使用して設定されている仮想アプライアンスに主に関連しています。

ログの例を次に示します。

```
Thu Jun 23 16:16:07 2022 Critical: Initialization of smart agent service failed. Reason : Port 65501 is any attempts to swap ports using the defined command will fail.
```

この問題を解決するには、CLIでversionコマンドの出力をチェックし、CPUの数と割り当てられたメモリがexpectedに設定されていることを確認します。

アプライアンスでサポートされるコアが増えている場合は、割り当てを修正します。

ライセンスクラウドからの応答が無効です

デバイスがSmart License Managerポータルから削除されている場合、古いバージョンでは次のエラーが返されます。

```
Thu Nov 15 13:50:20 2022 Warning: Failed to renew authorization of the product with Smart Software Mana
```

この問題を解決するには、アプライアンスを再登録してください。

有効なSSL証明書が送信されませんでした

このエラーがアプライアンスに表示され、アップデートを取得できない場合は、『[Field Notice:FN72502](#)』で詳細を参照してください。

```
21 Aug 2023 14:03:04 +0200 Unable to connect to the Cisco Aggregator Server.  
Details: No valid SSL certificate was sent
```

従来のVLN証明書ファイルには、更新やアップグレードにアクセスするためにTalosキーマスターによって作成された証明書が含まれています。古いキーマスター認証局(CA)の期限が2023年1月13日に切れました。

2021年12月15日より前に発行された証明書を含み、有効期間が12カ月を超えるVLN証明書ファイ

ルは、2023年1月13日より前に更新および適用する必要があります。

この問題を解決するには、シスコのライセンスサポートに連絡して、新しいVLNファイルを入手してください。

機能がコンプライアンス違反に移行しました

一部の機能がコンプライアンス違反に移行したログが表示された場合は、次の項目を確認してください。

1. 有効なライセンスがある
2. アプライアンスがスマートライセンスサーバに接続されている（この記事の「通信の要件」セクションを参照）
3. スマートライセンスログで、問題の詳細を確認します。
4. シスコサポートに連絡して支援を求める

サンプル ログを以下に示します。

```
Mon Sep 4 20:41:09 2023 Warning: Secure Web Appliance HTTPs Decryption license has been moved to Out of  
Mon Sep 4 20:41:10 2023 Warning: The Secure Web Appliance HTTPs Decryption is in Out of Compliance (00C
```

スマートエージェントが認証期限切れ状態

「Smart Agent is in Authorization Expired state」という重大なエラーが表示された場合は、次の行を参照して、この状態の理由を調べてください。

次にエラーの例を示します。

```
Fri Aug 18 15:51:11 2023 Critical: Web Security Appliance Cisco Web Usage Controls feature will stop wo
```

接続を確認し、デバイスがスマートライセンスポータルに登録されていることを確認してください。

参考

[Cisco Webセキュリティアプライアンスのベストプラクティスガイドライン - Cisco](#)

[BRKSEC-3303\(ciscolive\)](#)

[AsyncOS 14.5 for Cisco Secure Web Appliance ユーザガイド - GD \(一般導入\) - \[Cisco Secure Web Appliance\]の接続、インストール、および設定 - Cisco](#)

[Cisco Smart Software Manager - シスコ](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。